SORCHIC: Second Order Reversible Cellular Automata based Hybrid Image Cipher for IoT applications

Vijaya Bhaskara Rao
Manipal University Jaipur
Umashankar Rawat
Manipal University Jaipur
Satyabrata Roy
satya2k6ster@gmail.com
Manipal University Jaipur
Chhagan Lal
NTNU, Norway

Research Article

Keywords: Cellular Automata, Chaotic Map, Hybrid Image Cipher, IoT, Image encryption

Posted Date: August 30th, 2024

DOI: https://doi.org/10.21203/rs.3.rs-3969055/v2

Additional Declarations: The authors declare no competing interests.

SORCHIC: A Hybrid Image Cipher for IoT Applications using Second Order Reversible Cellular Automata

B VIJAYA BHASKARA RAO[1], UMASHANKAR RAWAT(MEMBER, IEEE)[2], SATYABRATA ROY (SENIOR MEMBER, IEEE)[3] AND CHHAGAN LAL(SENIOR MEMBER, IEEE)[4].

[1]Department of Computer Applications, Manipal University Jaipur, Rajasthan, India (e-mail: bvb.rao@gmail.com)
[2]Department of Computer Science and Engineering, Manipal University Jaipur, Rajasthan, India (e-mail: umashankar.rawat@jaipur.manipal.edu)
[3]Department of Computer Science and Engineering, Manipal University Jaipur, Rajasthan, India (e-mail: satyabrata.roy@jaipur.manipal.edu)
[4]Dept. of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway (e-mail: chhagan.lal@ntnu.no)

Corresponding author: Chhagan Lal (e-mail:chhagan.lal@ntnu.no).

ABSTRACT In the rapidly evolving digital world, ensuring secure data transmission, especially in image data pivotal to modern communication, remains critical. The rise of the Internet of Things (IoT) increases the demand for encryption systems that combine strong security with efficiency. However, many current cryptosystems tend to favor one aspect over the other. To resolve this, new algorithmic methods are being developed to find a balance. First Order Cellular Automata (FOCA) are particularly promising for image encryption, as they align well with the complexities of image processing while keeping implementation complexity simple. This paper presents SORCHIC, an novel hybrid encryption algorithm crafted specifically for IoT applications that encrypt multichannel images. Utilizing Second Order Cellular Automata (SOCA) and Chaotic Maps, SORCHIC is thoroughly examined in this study. We provide detailed insights into its mechanisms, followed by a thorough experimental analysis comparing it to existing encryption methods. The results highlight SORCHIC's robustness against various cryptanalytic attacks and demonstrate its superior efficiency over traditional techniques. This research advances encryption methods, particularly for IoT, by offering a robust, efficient, and secure solution for image data transmission.

INDEX TERMS Cellular Automata, Chaotic Map, Hybrid Image Cipher, IoT, Image encryption.

I. INTRODUCTION

In today's world of digital communication, an enormous volume of data, including images, flows through global networks daily. This data transmission is crucial for various sectors, such as the Internet of Things (IoT), social media, defense, and navigation, among others [1], [2]. Since the channels used for data transfer are frequently insecure and vulnerable to numerous threats, protecting this data has become essential to ensure the reliability of our communication systems [3].

Securing data transmitted over these channels is accomplished using encryption techniques [4], [5]. As most digital data transfer occurs through images, image encryption is fundamental to modern digital networks. In IoT applications, lightweight ciphers are essential due to the specific deployment features of these domains. Common methods for general image encryption include meta-heuristics, DNA encoding [6], Chaotic Maps [7], and FOCA. While some existing techniques offer strong protection against risks, others excel in encryption efficiency. Despite their strengths, achieving the ideal balance between robustness, efficiency, and low resource consumption remains a challenge. This balance is crucial to meet the diverse and evolving demands of the industry.

In our current research, we introduce a novel approach to image encryption, referred to as SORCHIC. This new method combines Chaotic Maps and Cellular Automata (CA) within a hybrid encryption framework. At the heart of this technique is the SOCA, which plays a crucial role in the encryption process. Additionally, it utilizes the complex scrambling capabilities of Chaotic Maps to enhance its resistance against differential attacks. A unique shuffling mechanism, distinguished by its key attributes, is integrated into this framework as part of the Chaotic Map component, offering unprecedented flexibility in design. Incorporating SOCA im-

proves the quality of encrypted images significantly, representing a notable departure from traditional ciphers based on FOCA.

A number of analyses of SORCHIC have been performed which demonstrate its efficacy as a cipher as well as its relative efficiency on standard input images compared to existing ciphers. The results of the analyses have been tabulated along with a comparison with some of the existing techniques in the Results Section V. The key contributions of the present work has been outlined below:

- A novel image cipher using SOCA and Chaotic Maps called SORCHIC is proposed. The technique is greatly compatible for implementation in IoT applications and is lightweight.
- A novel Chaotic Map is used for enhancement of the confusion characteristics of the cipher, making it robust against differential attacks.
- The results of the cryptanalysis of the resulting cipher prove the robustness of the cryptosystem against a wide array of attacks as well as highlight its efficiency for standard input images.

The subsequent sections of this document are structured as follows: In Section II, we explore the existing literature about the domain within which our present work resides. It is pivotal to contextualizing our research. Following this, in Section III, we concisely elucidate the fundamental concepts and architectural underpinnings that form the bedrock of the SORCHIC scheme. Understanding these prerequisites is instrumental in grasping the intricacies of our design. The crux of our contribution is unveiled in Section IV, where we offer an in-depth exposition of the SORCHIC scheme. This section provides a comprehensive view of our proposed system, its intricacies, and its design rationale. Moving forward, Section V serves as the platform for the presentation and analysis of the experimental results, accompanied by a comparative evaluation vis-a-vis existing techniques. This critical examination illuminates the efficacy of our approach. Lastly, Section VI offers insights into potential avenues for future research both within the scope of our current work and in broader contexts. It serves as a bridge to future developments and scholarly exploration.

II. RELATED WORKS

Image encryption, now a days has become an interesting topic and has drawn curiosity of many researchers. The image encryption schemes have been changed as per requirement of application and implementation hardware from time to time.

Researchers, such as Dong *et al.*, have ventured into harnessing the power of elementary Cellular Automata (CA) to amplify the chaotic properties inherent in systems like the Chirikov standard map-based "pseudo-random coupled map lattices (PRCML)" [8]. Their innovative approach yielded an image encryption scheme that boasts irreversibility and nonlinearity. Notably, they incorporated a dynamic S-box into their design, further enhancing the efficiency of the encryption scheme. Another trailblazing endeavor in this domain comes from Wang *et al.* [9], who crafted an image cipher grounded in reversible CA and block theory. Their methodology involved a combination of diffusion and confusion operations to scramble pixel data within input images. To fortify their scheme against a myriad of attacks, they employed SHA-256 with a 2D logistic map to generate initial seeds.

Meanwhile, Babaei *et al.* embarked on an intriguing journey, employing DNA sequences in conjunction with recursive CA to fashion a novel permutation and diffusion-based image cipher [10]. This innovative approach divided the encryption process into two distinct phases: permutation and diffusion. In the permutation phase, they harnessed the power of a logistic map. In contrast, the diffusion phase saw a synergy between DNA sequences and CA, creating a robust and dynamic encryption method. Arab *et al.* ventured into the world of image encryption with their unique approach [11]. Their design leveraged the Henon and Logistic maps, employing hyper-chaotic sequences to yield a substantial key space, heightened key sensitivity, and superior encryption speed. In this ever-evolving landscape of cryptography, researchers continue to explore innovative ways to infuse perplexity and burstiness into their algorithms, pushing the boundaries of security and encryption.

Hao *et al.* [12] developed a lossless image cipher based on CA and set partitioning in hierarchical structures. The cipher composed of compression process followed by three rounds of diffusion and scrambling. It achieved higher resistance towards common attacks and also passed the SP800-22 tests. Wang *et al.* [13] used quaternion algebra to design encryption of multiple RGB images at once. The scheme used multiple phases followed by an image phase mask in the end to add extra security features. The encryption framework proposed by Jasra *et al.* exemplifies the seamless integration of cutting-edge cryptographic principles and the intricate dynamics of hyperchaotic systems, thereby creating a security solution that boldly withstands a variety of threats. This sentiment resonates across the broader research landscape. A pivotal facet that distinguishes this scheme lies in their astute deployment of a novel 4D hyperchaotic system for permutation. This strategic choice imparts a heightened degree of non-periodicity, transforming the encryption process into an exquisite dance of entropy. Furthermore, it is intriguing to observe that the integration of chaotic systems, woven intricately with other sophisticated cryptographic techniques, has ignited the imagination of researchers across the globe [14]–[17].

Researchers have extensively explored chaos theory and cellular automata, yielding innovative approaches that challenge conventional encryption paradigms. Chai *et al.* [18] embarked on a pioneering journey, unveiling a technique that intertwines the enigmatic realm of chaotic maps with the realms of elementary cellular automata (CA) and blocks compressive sensing. The core of their approach involves a multi-stage process, comprising a sequence of transformations utilizing the Discrete Wavelet Transform (DWT), block

creation, scrambling, and compression of various blocks. What sets this technique apart is its reliance on the SHA256 hash of the plain image to generate the initial input values for the chaotic function. This ingenious twist bestows upon it a formidable resistance against cryptanalysis attacks, forging new frontiers in data security.

Concurrently, Choi *et al.* [19] traversed the complexities of encryption methodologies by leveraging the capabilities of a 3D chaotic cat map in tandem with the "programmable complemented maximum length CA (PC-MLCA)". The judicious selection of PC-MLCA endowed their system with hardware-friendly implementation and fortified it against the tempestuous storms of noise and various attacks. It is a testament to the fusion of chaos and computation. Naskar *et al.* [20] embarked on a quest to create a cryptosystem that could stand against the fiercest of adversaries. Their masterpiece leveraged the chaotic tent map and cellular automata, an alliance capable of generating cipher images with unparalleled robustness. The heart of their cryptosystem lay in the strategic use of variable-length block sizes and variable-length key streams derived from a 64-bit key and the plain image. This symbiosis rendered the cryptosystem exquisitely sensitive to the nuances of the plain image while erecting a formidable bulwark against myriad cryptographic assaults.

In recent years, the field of image encryption has witnessed a surge of innovative cryptosystems that harness the power of hyperchaos [21]–[23] in tandem with deep learning and DNA encoding [24]–[26]. For a comprehensive overview of various techniques for designing secure color image ciphers, one can delve into the insightful work of Ghadirli and Kaur [27], [28], where they painstakingly dissect and compare state-of-the-art strategies, scrutinizing their pivotal security attributes.

Many of these cryptographic endeavors employ a multifaceted approach, incorporating multiple iterations of pixel scrambling, confusion, diffusion, shuffling, and other intricate operations to fortify the resilience of their ciphered images. However, while enhancing the cipher's robustness, this multifarious approach concurrently inflates its implementation's complexity and demands substantial computational resources. In stark contrast, the groundbreaking *proposedscheme* presented herein diverges from convention by utilizing chaotic maps once in the encryption process, subsequently relying predominantly on SOCA to generate ciphered images. Remarkably, this innovative approach does not compromise the integral security features paramount in image encryption.

III. PREREQUISITES

In the next section, we will explore the mathematical foundations and frameworks crucial to the architecture of our SORCHIC . We begin by laying a basic groundwork in Cellular Automata (CA) and delving into the engrossing area of Chaotic Maps. These foundational concepts will pave the way for a detailed analysis of the SORCHIC cryptosystem, which will be thoroughly presented in the following section.

A. CELLULAR AUTOMATA

Cellular Automata has a rich history dating back to the early 1950s, with John Von Neumann pioneering their study as powerful computational models [29]. These models serve as intricate representations that simulate the intricate behavior of real-world systems, emphasizing localized influences on behavior. This emulation is achieved through the elegant concept of automata represented as spatial structures resembling a grid of individual cells. In this framework, each cell's state's evolution hinges solely on its neighboring cells' values. Take, for instance, a 2-Dimensional Cellular Automaton (2D CA): At any given time step 't', the state of a cell at coordinates (x, y) in the grid evolves to its state at time $(t + 1)$, with this transformation being entirely reliant on the values held by its adjacent cells.

Two fundamental cell neighborhoods emerge as key players in cellular automata: the renowned "Von Neumann Neighborhood" and the comprehensive "Moore Neighborhood". Understanding these neighborhoods is pivotal in exploring the dynamics of cellular automata systems. The "Von Neumann Neighborhood" encompasses a set of cells surrounding a central cell (x, y), comprising the cardinal directions: $(x-1, y)$ to the north, $(x+1, y)$ to the south, $(x, y-1)$ to the west, and $(x, y + 1)$ to the east. This restricted neighborhood encapsulates the immediate surroundings of the focal cell. In contrast, the "Moore Neighborhood" expands upon this concept by embracing a broader perspective. In addition to the cardinal directions, it includes the diagonal cells: $(x - 1, y-1)$ to the northwest, $(x-1, y+1)$ to the northeast, $(x+ 1, y-1)$ to the southwest, and $(x+1, y+1)$ to the southeast, encompassing all eight adjacent cells around (x, y). This extended neighborhood offers a more comprehensive view of the cellular environment, considering both the immediate and diagonal neighbors. To visualize these neighborhoods, refer to Figure 1 below, illustrating the cells constituting the "Von Neumann" and "Moore Neighborhoods". Understanding the distinctions between these two cell neighborhoods is pivotal in studying cellular automata, as they influence the dynamics and behavior of these intriguing computational systems.

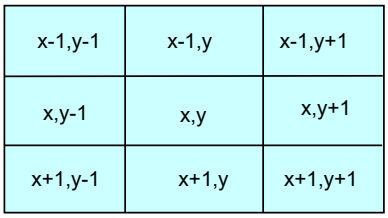


FIGURE 1: Moore Cellular Automata

In the complex world of cellular automata (CA), behavior in finite grids reveals a striking contrast. This complexity arises from the unique neighborhood conditions at the grid's edges, which differ from the uniform conditions within the grid. To address this, two commonly used boundary conditions are employed: periodic and null boundary condi-

tions [30]. The null boundary condition replaces border cells with '0' or a null value, which simplifies the grid but may overlook some neighbor interactions. On the other hand, the periodic boundary condition treats the grid as if it were wrapped into a torus. This approach connects the borders with the interior, allowing all neighbors to influence the cellular automaton's behavior at each step. The selection of these boundary conditions significantly impacts the complex behavior of cellular automata in finite grids.

Cellular Automata (CA) architectures include a variety of computational models, each with distinct features that determine how they operate. The specific CA architecture we previously discussed is part of the FOCA category, which is unique in that each cell's state is influenced only by the prior states of its neighboring cells. Essentially, at any given time step t, a cell's state is determined by looking at the states of its adjacent cells at the previous time step $(t-1)$. This principle forms the core of FOCA and its computational rules [31]. Expanding on this idea, some CA systems exhibit more complex behavior by incorporating memory, meaning that their current state depends not only on the previous time step's neighbors but also on the states of cells from earlier time steps. This memory function allows these systems to predict or calculate future states more effectively, as they can retain information over multiple time steps, enhancing their predictive accuracy.

In the realm of Cellular Automata (CA), and specifically Second Order Cellular Automata (SOCA), we encounter a situation where a cell's state at time t depends not just on the state at time $(t-1)$ but also on the state at time $(t-2)$. This dual dependence creates a fascinating area of computational dynamics, as shown in Figure 2. Building on this concept, Third Order Cellular Automata (TOCA) introduce even more complexity. In TOCA, a cell's state at time t depends on the states at times $(t-1)$, $(t-2)$, and $(t-3)$. This three-state dependence increases the complexity of CA systems, offering numerous opportunities for exploration and analysis. Our work focuses on the dynamics of SOCA, where the richness of these interactions promises to reveal new insights and challenges in the study of cellular automata.

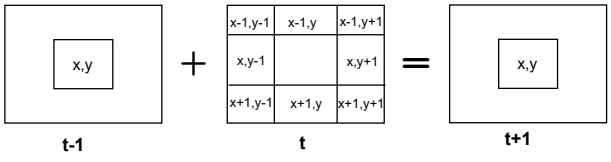


FIGURE 2: Second Order Cellular Automata

B. CHAOTIC MAPS

Chaotic Maps are, in essence, maps (or functions) defined usually in terms of a system of equations that exhibit chaotic behavior. In other words, these are highly sensitive to input conditions [32]. These equations are evaluated recursively over the inputs such that the output for the current state becomes the input for the next.

Many chaotic maps are widely used in the field of cryptography because of their desirable characteristics of producing highly randomized states which vary dramatically with slight changes in inputs. Some of the widely used Chaotic Maps include the Arnold's Cat Map, Logistic Map, Lorenz Map etc. These maps also have the useful property of being periodic, or repeating states. This can be utilized in designing reversible systems where we want to return to the original state of the system as is done in Encryption schemes.

In the present work, a Tinkerbell map is presented and used in the system architecture of the SORCHIC scheme. A function is used in dynamical systems to explain the time dependence of any point geometrically. Tinkerbell map is an example of similar discrete system that is mathematically expressed by Equation (1) and (2). Figure 3 shows the behavior of this map.

$$p_{n+1} = {p_n}^2 - {q_n}^2 + ap_n + bq_n \tag{1}$$

$$q_{n+1} = 2p_nq_n + cp_n + dq_n \tag{2}$$

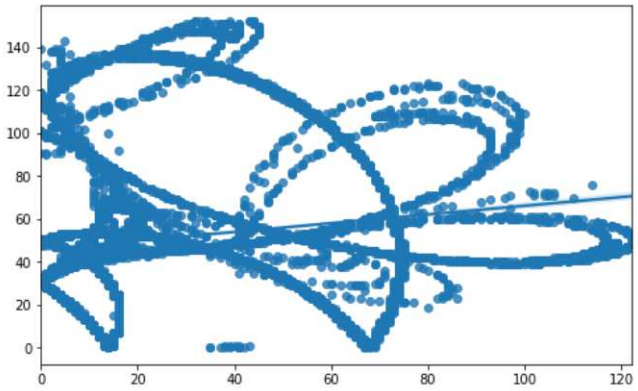


FIGURE 3: Tinkerbell map [33].

Equation (1) and (2) contain 4 coefficients represented as a, b, c and d [34] which are constants.

IV. SORCHIC - THE PROPOSED TECHNIQUE

The proposed encryption method uses a symmetric cipher design that incorporates elements from diverse cryptographic approaches. At its core, the algorithm employs a hybrid structure comprising three main phases. Initially, it breaks down the input image into its RGB components. Then, each of these channels undergoes encryption separately using the cipher algorithm, and their outputs are combined to create the final encrypted image. The algorithm's tripartite framework consists of phases for key generation, state evolution, and shuffling. The key generation phase occurs once during initialization to set up inputs for subsequent stages. Following this, the state evolution and shuffling phases operate in sequence over a fixed number of iterations. Notably, the

output from each iteration feeds into the next, forming a continuous iterative process that concludes with the creation of the encrypted image and decryption key. Figure 4 provides a visual representation of this intricate process.

A. KEY GENERATION PHASE

In the beginning of this process, a critical step occurs: creating a crucial image, which relies on using a seed vector as input. This pivotal image precisely matches the dimensions of the input image. The seed vector, composed of pixels arranged in a grid pattern, appears randomly and has dimensions of $M \times M$, where M must evenly divide the dimensions of the input image, referred to as dim$\times$ dim. This requirement ensures the pivotal image aligns perfectly with the input dimensions, achieved through a careful tiling process using the seed vector. The value of M can vary, as long as it remains a divisor of dim. This initial phase produces the pivotal output known as the key image, essential for subsequent stages of the process. Interestingly, while the outlined tiling method reliably generates a key image for encryption, practicality allows for almost any image to serve this role, provided it matches the dimensions of the input image. Further details on the intricate process of key generation can be found in Algorithm 1.

Algorithm 1 Key Generation Algorithm

Input: Seed Vector V of dimension $M \times M$
Output: Key Image K of dimension $dim \times dim$

for $x \leftarrow 0$ to $dim - 1$ **do**
  for $y \leftarrow 0$ to $dim - 1$ **do**
    $i \leftarrow 0$
    $j \leftarrow 0$
    for $i \leftarrow 0$ to $m - 1$ **do**
      for $j \leftarrow 0$ to $m - 1$ **do**
        $K[x + i][y + j] \leftarrow V[i][j]$
      end for
    end for
    $y \leftarrow y + m$
  end for
  $x \leftarrow x + m$
end for

B. STATE EVOLUTION PHASE

The core of this algorithm represents its distinctive feature, standing at the forefront of its uniqueness. This pivotal phase introduces the SOCA (State-Of-the-Cellular-Automaton) structure, which orchestrates the primary encryption process. In this stage, the algorithm takes two essential inputs: the RGB channels of the input image and the key image generated in the preceding phase, which serve as the states T_0 and T_1 for the subsequent encryption computation. The proposed algorithm adopts a Moore Neighborhood SOCA configuration, operating within a framework of periodic boundary conditions to execute the encryption. The equation that governs the derivation of the next states is elegantly presented below:

$$T_{i,j}^{n+1} = XOR_{Moore}^{Periodic}(T_{i,j}^{n},\, T_{i,j}^{n-1}), \tag{3}$$

Considering the function $XOR_{Moore}^{Periodic}(T(n))$, which yields the result of performing an XOR operation on the Moore neighborhood surrounding the cell at coordinates (i, j) within the SOCA. This neighborhood comprises all adjacent cells to the state $T(n)$ except for the cell at (i, j). The procedure involves the repetition of this XOR operation for a fixed number of iterations, resulting in a series of output states. The $XOR_{Moore}^{Periodic}$ function, central to the SOCA process, can be described as follows:

$$\begin{aligned} XOR_{Moore}^{Periodic}(T_{i,j}^{n}) = T_{(i-1+dim)\%dim,j} \\ \oplus T_{(i+1)\%dim,j} \oplus T_{i,(j-1+dim)\%dim} \\ \oplus T_{i,(j+1)\%dim} \oplus T_{(i-1+dim)\%dim,(j-1+dim)\%dim} \\ \oplus T_{(i+1)\%dim,(j-1+dim)\%dim} \\ \oplus T_{(i-1+dim)\%dim,(j+1)\%dim} \\ \oplus T_{(i+1)\%dim,(j+1)\%dim} \end{aligned} \tag{4}$$

The XOR function emerges as a potent tool. It capitalizes on an interesting property: when $a \oplus b = c$, the inverse also holds, $b \oplus c = a$. This intrinsic characteristic unveils a remarkable symmetry, rendering the decryption process a mirror image of its encryption counterpart. As we traverse further into this intricate procedure, the outputs of this stage come to the forefront. These outputs are not singular but a pair, representing both the $(x + 1)^{th}$ and the x^{th} images. This duality, arising after x steps of computation, forms the foundation for the subsequent phase.

C. SHUFFLING PHASE

This phase, as the name suggests, shuffles the output of the previous stage using a Tinkerbell map to introduce high level of differentiation in the output and to maintain the practicality as well as flexibility of implementation of the scheme itself. The working of this phase is shown in Algorithm 2. The output of this stage are the shuffled images T'_{x+1} and T'_x corresponding to the output images T_{x+1} and T_x of the previous stage.

D. STRUCTURE OF SORCHIC

The heart of the encryption process lies in the complex interaction of phases that evolve over time. Over a series of t iterations, these phases work together to produce two critical outcomes: the encrypted image and the decryption key representation. This encryption process, utilizing techniques like shuffling and SOCA, is detailed in Algorithm 3. Conversely, Algorithm 4 explains the decryption counterpart, emphasizing the intricate symmetry between Encryption and Decryption in their structural design. Figure 4 elegantly illustrates the architectural framework of the SORCHIC scheme,

Algorithm 2 Shuffling Algorithm

Input: Output Image C of previous phase
Output: Shuffled Image C'

for $x \leftarrow 0$ to $dim - 1$ **do**
  for $y \leftarrow 0$ to $dim - 1$ **do**
    $i1 \leftarrow i^2 - j^2 + a \times i + b \times j$
    $j1 \leftarrow 2 \times i \times j + c \times i + d \times j$ ▷ New indices are computed using Tinkerbell map
    $C'[i][j] \leftarrow C[i1][j1]$
  end for
end for
$C \leftarrow C'$

visually capturing the harmonious interaction of these cryptographic processes. During decryption, the "Decryption Key Image" functions as the Initial Vector (IV), and the encrypted image serves as the "Input Image," as depicted in Figure 4.

Algorithm 3 Encryption Algorithm

Input: Input Image I, Key K, Number of Iterations, p
Output: $Cipher_{Image}$, Decryption Key Image

$iter \leftarrow p$
$C_0 \leftarrow I$
$C_1 \leftarrow K$
$C2 \leftarrow$ Initialize with 0
for $x \leftarrow 0$ to $iter - 1$ **do**
  for $i \leftarrow 0$ to $dim - 1$ **do**
    for $j \leftarrow 0$ to $dim - 1$ **do**
      $C2[i][j] \leftarrow XOR_{Moore}^{Periodic}(C1) \oplus C_0[i][j]$ ▷ Using the $XOR_{Moore}^{Periodic}$ function in equation 4
    end for
  end for
  if $x + 1\%p == 0$ **then**
    $C2 \leftarrow$ shuffle(C2) ▷ Using the Shuffling procedure shown in Algorithm 2
    $C_1 \leftarrow$ shuffle(C1)
  end if
  $C_0 \leftarrow C_1$
  $C_1 \leftarrow C2$
end for

V. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the analysis of the proposed scheme as well as a summarized comparison to some of the existing techniques of similar design. The following experiments have been performed on a Google Compute Engine with 12.68 GB RAM and 107.72 GB storage. Constant values for the various algorithm hyper-parameters have been used throughout the analysis of the scheme. These parameters include the number of SOCA iterations p and image dimension dim.

These values can be varied based on the robustness, efficiency and sensitivity requirements. The Boat image is used as key image instead of the aforementioned key generation procedure in order to showcase the performance

Algorithm 4 Decryption Algorithm

Input: $Cipher_{Image}$ C, Key K, SOCA Iterations p
Output: Original Image

$iter \leftarrow p$
$C_0 \leftarrow C$
$C_1 \leftarrow K$
$C2 \leftarrow$ Initialize with 0
for $x \leftarrow 0$ to $iter - 1$ **do**
  if $x\%p == 0$ **then**
    $C_1 \leftarrow$ shuffle(C_1)
    $C_0 \leftarrow$ shuffle(C_0)
  end if
  for $i \leftarrow 0$ to $dim - 1$ **do**
    for $j \leftarrow 0$ to $dim - 1$ **do**
      $C2[i][j] \leftarrow XOR_{Moore}^{Periodic}(C1) \oplus C_0[i][j]$
    end for
  end for
  $C_0 \leftarrow C_1$
  $C_1 \leftarrow C2$
end for

and robustness of the scheme in the absence of externally induced randomness. “Boat", “Baboon" and “Peppers" had been considered as plain images for various experiments. The corresponding enciphered and deciphered images are presented in Figure 5.

A. HISTOGRAM ANALYSIS

Studying the Histograms of Input and Cipher Images provides valuable insights into how pixel distributions differ between these two distinct sets. Ideally, we would expect significant differences in the histograms, indicating that pixel intensity values are markedly different between the two types of images. However, real-world images often have non-uniform histograms due to smooth transitions between nearby pixels. In contrast, cipher images typically exhibit more uniform histograms, suggesting abrupt changes between neighboring pixel groups. This characteristic is crucial for secure image encryption. Refer Figure 6, 7, 8 for a graphical depiction of these histograms for cipher images across their RGB color channels. Similar uniform visual representations were generated for all test images.

B. INVESTIGATION OF CIPHER IMAGE QUALITY

In this section, we carefully analyze the image quality achieved by SORCHIC. Our evaluation will use three important and well-established metrics, namely “Mean Square Error (MSE)", “Peak Signal-to-Noise Ratio (PSNR)" and “Mean Absolute Error (MAE)". The formulae for computing these values can be found in [35]. A comparison of the values between SORCHIC and existing popular techniques is presented in Table 1.

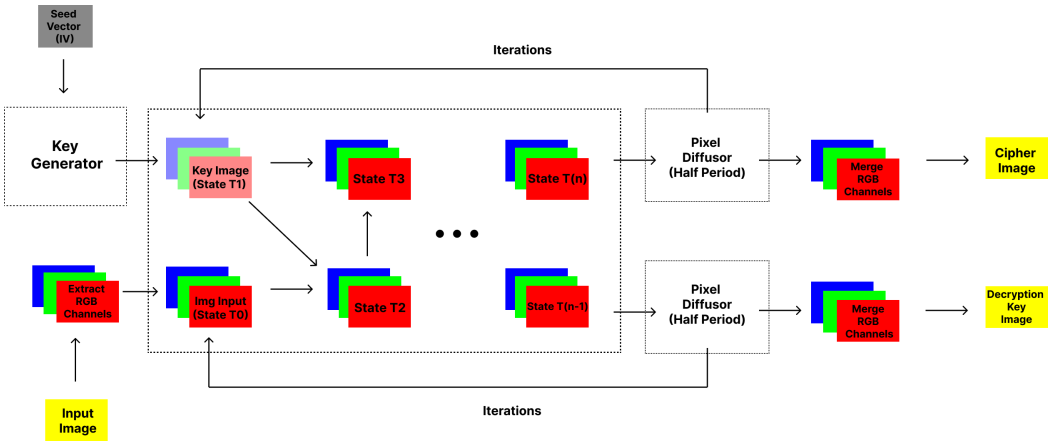


FIGURE 4: SORCHIC Architecture

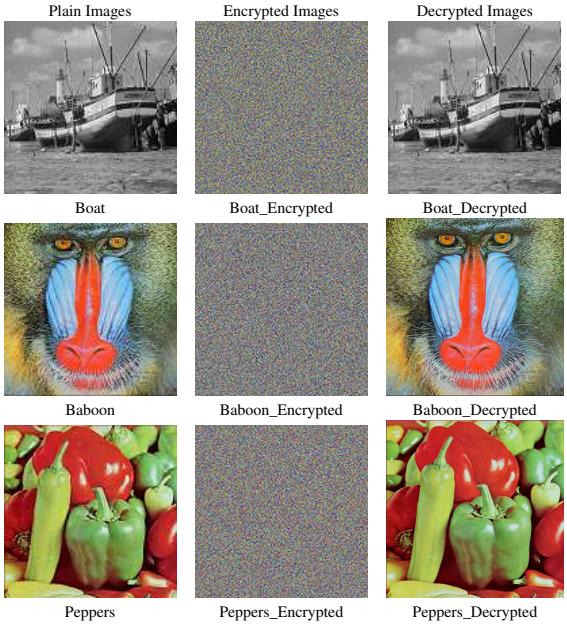


FIGURE 5: Input and Result Images using SORCHIC

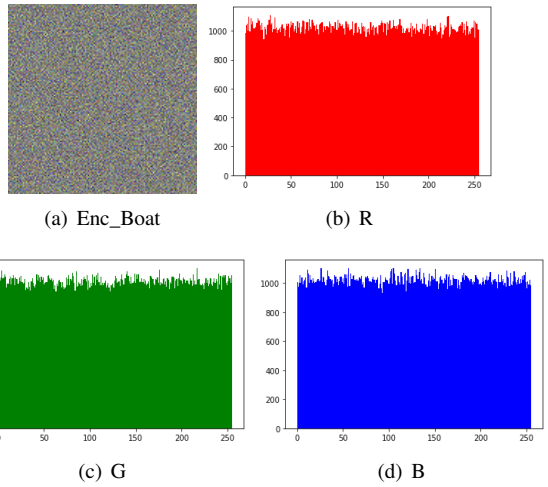


FIGURE 6: Channel-wise histograms of Boat generated by SORCHIC

TABLE 1: Comparison of Cipher Image quality using various parameters

	MSE		PSNR		MAE	
Methods	Baboon	Pepper	Baboon	Pepper	Baboon	Pepper
Ref. [36]	11143.49	10784.50	7.661	7.803	88.344	84.828
Ref. [37]	9368.70	11158.19	8.42	7.67	79.28	86.27
Ref. [38]	7,364	8,319	9.4598	8.93		
SORCHIC	11149.36	10845.41	8.593	8.176	89.237	87.572

C. ANALYSIS OF AVALANCHE EFFECT

This analysis demonstrates how sensitive the SORCHIC is to the experiment's secret key. It shows that even a tiny change to the secret key can completely render the restored image unintelligible [39].

Alternatively, the changed key will bring forth an entirely dissimilar cipher image. Figure 9 presents some decrypted images produced as a consequence of only one rule change in the secret key.

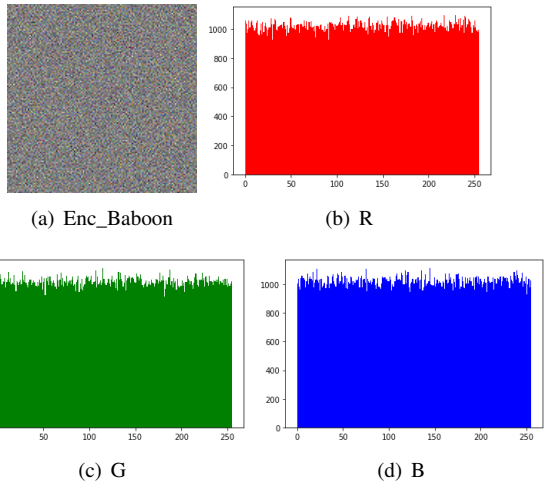
TABLE 2: Comparative analysis of key-sensitivity (%)

Image	**SORCHIC**	PVCA [40]	Babaei *et al.* [10]
Baboon	99.76	99.76	99.60
Peppers	99.72	99.71	99.66

It is clear that the system is extremely sensitive to the secret key. The comparison between SORCHIC and its counterparts is given in Table 2. Clearly, the proposed technique outperforms the existing ones.

D. RESISTANCE AGAINST STANDARD ATTACKS

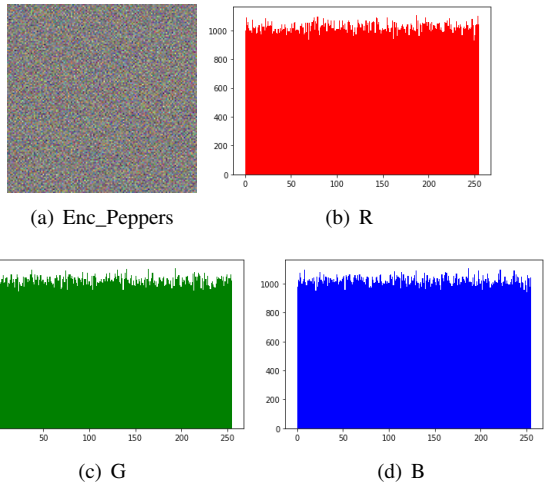
SORCHIC is a symmetric image cipher which encodes an image based on SOCA rules as written in Section IV. This is designed by "Moore neighborhood periodic boundary" second order CA that changes its configuration based on nine neighbors dynamically. Here, 3 crucial parts are selected randomly – (1) Key, K (2) SOCA iteraions, p and (3) the



(a) Enc_Baboon (b) R

(c) G (d) B

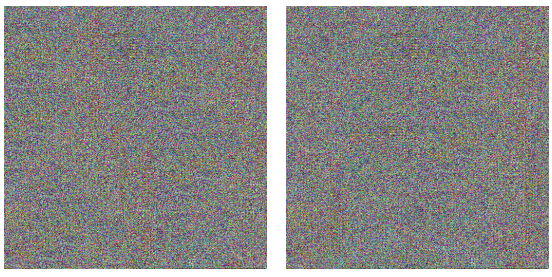
FIGURE 7: Channel-wise histograms of Baboon generated by SORCHIC



(a) Enc_Peppers (b) R

(c) G (d) B

FIGURE 8: Channel-wise histograms of Peppers generated by SORCHIC



(a) Recovered Baboon (b) Recovered Peppers

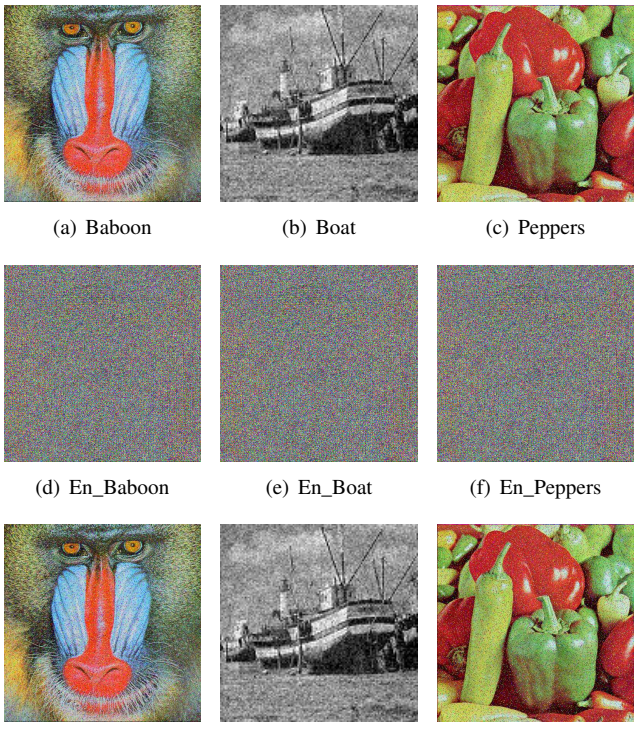
FIGURE 9: Decryption results with altered key

epochs, w for which rounds the method should to be run. As a result, the cipher images possess high randomness.

Additionally, this approach can produce entirely various types of cipher images from very similar initial image types. To put it another way, a single original image can bring forth a variety of cipher images based on the three critical parts mentioned above. Additionally, even if the same K component is considered, the encoded images will differ. This is because of the encryption method's capacity to achieve a high degree of confusion and diffusion qualities. Therefore, even if the original image pixels are replaced by all zero values, it prevents the opponent from learning anything useful. Thus, SORCHIC prevents chosen ciphertext, chosen plaintext, known plaintext and known ciphertext attacks.

E. ROBUSTNESS TEST AGAINST DIFFERENT NOISE LEVELS

To verify the resilience of the suggested approach, various noise levels are used. The plain images are first given a varying percentage of "Salt and Pepper" noise, after which they are encrypted and transferred to the recipient end. Here, En_Baboon and Re_Baboon refer to encrypted Baboon and Recovered Baboon respectively. Similarly other nomenclatures are used.



(a) Baboon (b) Boat (c) Peppers

(d) En_Baboon (e) En_Boat (f) En_Peppers

(g) Re_Baboon (h) Re_Boat (i) Re_Peppers

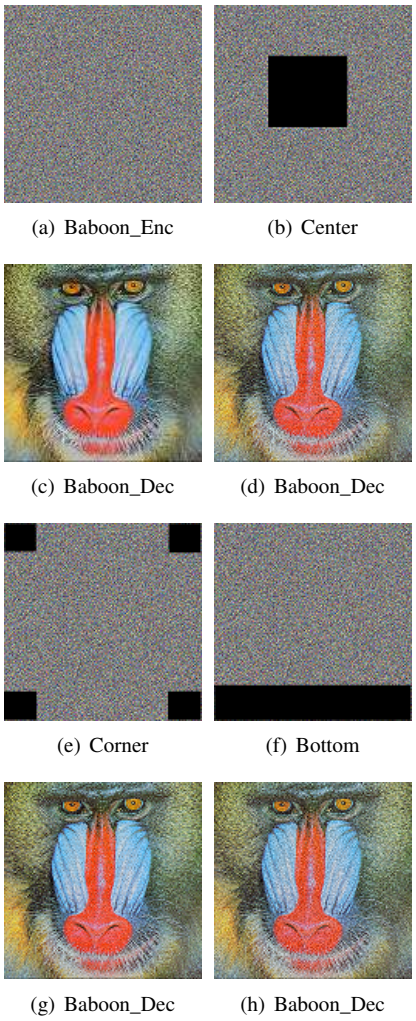
FIGURE 10: Robustness test with 10 % noise level for SORCHIC

The original images are deciphered at the receiver's end. Figure 10 displays the corresponding images with a 10% noise level. The figures unambiguously demonstrate that by looking at the recovered photographs, the plain images may be quickly identified.

F. DATA LOSS ANALYSIS

Images may be exposed to a variety of disturbances while being transmitted from one point to another. Data loss could arise at the receiver's end as a obvious consequence. Hence, the receiver can perceive something quite different. Even with a certain amount of data loss, the method must recover the actual image without losing its generality. To put it another way, the cipher must decipher and retrieve the plain image that closely resembles the original image.

In SORCHIC , we have checked data losses at various image coordinates as depicted in Figure 11. As observed in the figures, the reconstructed images had a strong resemblance with the original ones, thus supporting the strength of the suggested scheme.



(a) Baboon_Enc (b) Center

(c) Baboon_Dec (d) Baboon_Dec

(e) Corner (f) Bottom

(g) Baboon_Dec (h) Baboon_Dec

FIGURE 11: Data loss analysis of the Baboon encrypted image and decrypted image

G. EVALUATION OF INFORMATION ENTROPY

Entropy in information theory serves as a fundamental measure of randomness. Image encryption plays a pivotal role as a metric for quantifying the average information content stored within each bit of an image. When we examine a typical, unencrypted image, we observe a wide range of pixel values, leading to significant variations in the probability distribution of these values across the image. Conversely, pixel values tend to exhibit a uniform distribution in the realm of ideally encrypted images, where each possible value holds an equal probability. This state is often described as having higher entropy than the former scenario. To calculate the Information Entropy of an image, we utilize Equation 5 as our mathematical tool.

$$\gamma = \sum_{i=0}^{mn} P(T_i)(-\log_2 P(T_i)), \tag{5}$$

Here, the image dimensions are denoted as $m \times n$, capturing the fundamental scale of the image. Additionally, we refer to $P(T_i)$, which corresponds to the pixel value count in the image's histogram for each pixel value T_i [43]. In Table 4, we present a comparative analysis of the entropy values for encrypted versions of various images. These values serve as a crucial metric for assessing the quality of the encryption scheme under consideration. Upon closer examination of the entropy values, it becomes evident that the SORCHIC scheme yields commendable results. This observation underscores the scheme's resilience against various forms of randomness attacks, making it a robust choice for image encryption.

H. ASSESSMENT OF CORRELATION COEFFICIENTS

The Correlation Coefficient, denoted as μ, is a pivotal statistical metric in gauging the resemblance between two images. It fundamentally quantifies the extent of diversity exhibited by the pixel values within these two images. The Correlation Coefficient's value is constrained within $[-1, 1]$. Notably, a value nearing either extremity of this interval denotes an exceptionally pronounced likeness, whereas a value approximating '0' signifies a considerable dissimilarity. Mathematical expression for calculating the Correlation Coefficient is defined by Equation 6, as follows:

$$\mu = \frac{\sum_m \sum_n (X_{mn} - \bar{X})(Y_{mn} - \bar{Y})}{\sqrt{(\sum_m \sum_q (X_{mn} - \bar{X})^2)(\sum_m \sum_n (Y_{mn} - \bar{Y})^2)}}, \tag{6}$$

Here, $\bar{X}$ and $\bar{Y}$ represent the mean pixel values attributed to the images under scrutiny. These statistical aggregates are pivotal in unraveling the image intricacies. Meanwhile, X_{mn} and Y_{mn} denote the pixel values residing at the index (m, n), as detailed in the notable work by Roy et al. [40]. However, the crux of our investigation lies in the comparative analysis of μ values, a fundamental variable governing the encrypted images in different directions. We have meticulously curated a tabulated presentation encapsulated in Table 3 to shed light on this. This table is a valuable reference point for deciphering the nuances of the directional μ variations.

In image encryption, the vertical, horizontal, and diagonal spectrums of correlation are used to measure how well the

TABLE 3: Comparison of μ-Values generated through SORCHIC with recent methods

Methods	Baboon				Peppers			
	μ				μ			
	Horizontal	Vertical	Diagonal	Average	Horizontal	Vertical	Diagonal	Average
Ref. [38]	-0.003668	0.0003721	-0.0009163	-0.0014041	0.000127	0.0003223	0.0089575	0.0031356
Ref. [41]	-0.001100	-0.002037	0.00098	-0.0007204	0.00017	-0.001268	0.00044	-0.00022
Ref. [42]	0.0025	0.0064	0.0035	0.00413	-0.0020	0.00008	-0.0064	-0.002773
SORCHIC	0.000897	0.000124	-0.000068	0.0003177	0.00002	-0.00087	0.00099	0.00004667

TABLE 4: Comparison of entropy values with recent techniques

Scheme/Image	Baboon	Peppers
Ref. [38]	7.9974	7.9974
Ref. [41]	7.9993	7.9993
Ref. [42]	7.99907	7.99890
SORCHIC	7.99998	7.99995

encryption algorithm disrupts the inherent correlations in an image. Effective image encryption should result in low correlations across all these spectrums, indicating that the pixel values have been thoroughly randomized and the image is secure against attacks that exploit these correlations. As can be seen from Table 3, the values of μ are lesser for Baboon in horizontal spectrum as compared to Ref. [[42]]. On the other hand, majority of the values achieved are lesser than the existing algorithms, indicating the strength of the encryption algorithm.

I. DIFFERENTIAL ANALYSIS

Differential Attacks constitute a pivotal category of cryptanalysis techniques, wherein the input image undergoes slight perturbations and is subsequently subjected to encryption using the same cryptographic key in conjunction with the original unaltered image. Subsequently, a comparative analysis is performed between the original and perturbed input images' encrypted representations to elucidate the inherent relationships between these two encrypted forms. In cryptography, fortifying encryption mechanisms against such formidable attacks is paramount. It necessitates the implementation of cryptographic algorithms that exhibit a property where even a minute alteration in the input data results in a completely divergent encrypted output. The realization of such a property forms a fundamental goal in designing and evaluating cryptographic techniques.

TABLE 5: Comparison of differential analysis metrics of SORCHIC with existing schemes

Images	Baboon		Pepper	
Metrics	NPCR	UACI	NPCR	UACI
Ref. [38]	99.6384	33.6305	99.6628	33.5712
Ref. [41]	99.6081	33.4581	99.6095	33.4581
Ref. [44]	99.6105	33.4661	99.6078	33.4637
SORCHIC	99.9856	33.8712	99.9775	33.0220

Two critical parameters that play an instrumental role in quantifying the robustness of an encryption scheme in the context of differential attacks are "Number of Pixel Change Rate (NPCR)" and "Unified Average Changing Intensity (UACI)". These parameters serve as indispensable metrics, facilitating a comprehensive assessment of the encryption method's efficacy in thwarting differential attacks. Mathematically, these metrics can be expressed through the following equations:

$$\begin{cases} N(M_1, M_2) = \sum \frac{M(m,n)}{X \times Y} \times 100\%, \\ U(M_1, M_2) = \sum_{m,n} \frac{|M_1(m,n) - M_2(m,n)|}{R \times X \times Y} \times 100\%, \end{cases}$$

Here, X and Y symbolize the dimensions of the images, with R representing the uppermost attainable value for the image's pixels. The function $M(p, q)$ characterizes the disparity between the two images at position (p, q), a quantity computed via the utilization of Equation 7.

$$M(m,n) = \begin{cases} 0 & \text{if } M_1(m,n) = M_2(m,n); \\ 1 & \text{if } M_1(m,n) \neq M_2(m,n), \end{cases} \quad (7)$$

In the context of assessing the performance of the SORCHIC scheme, it becomes imperative to delve into a comparative analysis of the NPCR and UACI metrics when juxtaposed with various existing techniques. The results of this comparison are meticulously tabulated in Table 5, shedding light on the scheme's efficacy and differentiating it from its contemporaries.

J. NIST TESTS FOR RANDOMNESS

The security of any cryptographic cipher is heavily reliant on assessing its randomness. In the evaluation of the randomness of the proposed scheme (SORCHIC), we have employed the widely recognized SP800-22 suite [46], as established by the "National Institute of Standards and Technology (NIST)"[1].

These assessments focus on identifying various forms of non-randomness that may be present in a sequence. For each assessment, a standard significance level of α = 0.01 was applied when analyzing the P-values generated. A sequence is considered to have passed a statistical test if the P-value is greater than or equal to α; otherwise, it fails. The NIST recommends two methods for interpreting the results: evaluating

[1] https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic

TABLE 6: Comparison of NIST Randomness Test Results

Techniques	Ping *et al.* [45]			SORCHIC		
Size	512×512			512×512		
Tests	p-value	Z	Result	p-value	Z	Result
Serial (m=16, delsi2m)	0.834308	0.99	✓	0.932712	0.99	✓
Rank	0.275709	1	✓	0.275814	1	✓
Overlapping Templates	0.924076	0.97	✓	0.931456	0.97	✓
Longest Runs of 1s	0.987896	0.99	✓	0.987928	0.99	✓
Block Frequency (m=20000)	0.935716	0.98	✓	0.985423	0.98	✓
Non-overlapping Templates	0.554420	0.99	✓	0.555644	0.99	✓
Spectral DFT	0.897763	0.99	✓	0.901224	0.99	✓
Frequency	0.759756	1	✓	0.868268	1	✓
Maurer's Universal	0.075719	1	✓	0.094342	0.98	✓
Runs (Forward)	0.935716	1	✓	0.966725	1	✓
REV*	0.468595	1	✓	0.471738	0.99	✓
RE†	0.602458	1	✓	0.614245	1	✓
Linear Complexity (m=500)	0.236810	0.99	✓	0.329873	0.99	✓
Approximate Entropy	0.419021	0.98	✓	0.438003	0.98	✓
Cumulative Sums (Forward)	0.122325	0.98	✓	0.127881	1	✓

*REV = "Random Excursions Variant" (x = -1)
†RE = "Random Excursions" (x = -1)

the proportion of sequences that pass a test and examining the distribution of P-values.

1) Proportion of sequences:
The range of valid proportions can be defined as,

$$\hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}},$$

where, $\hat{p} = 1 - \alpha$, and m is the sample size [45]. If the proportion is not within this interval, it indicates that the data might not be random. For our situation where m = 100, the acceptable proportion range is 0.99 $\pm$ 0.02985, which translates to [0.96015, 1.01985].

2) Distribution of P-value:
To verify uniformity, the P-value distribution is examined. The range from 0 to 1 is segmented into 10 equal parts, and the calculations proceed as follows:

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - m/10)^2}{m/10},$$

were, F_i represents the frequency of occurrences where the P-value falls within sub-interval i, and m stands for the sample size. A P-value is computed so that

$$P{-}value = igamc\left(\frac{9}{2}, \frac{\chi^2}{2}\right),$$

Here, the incomplete Gamma function, denoted as igamc, is used to determine if a sequence is uniformly distributed. A P-value of 0.0001 or higher indicates that the sequence meets this criterion.

We analyze the randomness of the output sequence generated by our proposed algorithm. We tested 100 different sequences of cipher images, each 1,000,000 bits long, using the NIST STS (version 2.1.1). The results of these tests are recorded in Table 6, where Z represents the proportion. The findings confirm the strong performance of SORCHIC in all tests. As mentioned earlier, for this evaluation, we used a sample size of m=100 and considered p-values within the range of [0.96015, 1.01985].

VI. CONCLUSION

In the scope of this research endeavor, we introduce a pioneering image encryption framework known as SORCHIC. This innovative scheme harnesses the power of Second Order Cellular Automata (SOCA) in conjunction with Chaotic Maps to orchestrate the encryption process. Notably, our work introduces an entirely novel family of chaotic maps that underpins the overarching architecture of the SORCHIC. Its adaptability, manifest through incorporating diverse hyper-parameters in its design, sets this scheme apart. This adaptability grants it the dual prowess of robustness and efficiency, as these hyper-parameters can be facilely fine-tuned to yield the desired system performance. The rigor of our work extends to a comprehensive suite of cryptanalysis techniques, including Histogram Analysis, Cipher Image Analysis, Differential Analysis, and Information Entropy assessment. These meticulous examinations corroborate the SORCHIC's resilience against various security attacks, reinforcing its credentials as a stalwart guardian of digital imagery.

Looking forward, future research will explore the performance of SORCHIC across a range of hyper-parameter values to enhance robustness against adversarial attacks while optimizing efficiency. Additionally, an evolved version of SORCHIC will eliminate the need for key images, thereby improving practicality across various applications.

REFERENCES

[1] İ. Kahraman, A. Köse, M. Koca, and E. Anarım, "Age of information in internet of things: A survey," IEEE Internet of Things Journal, 2023.

[2] A. Hazra, A. Kalita, and M. Gurusamy, "Meeting the requirements of internet of things: The promise of edge computing," IEEE Internet of Things Journal, 2023.

[3] X. Wu, Z. Jing, and X. Wang, "The security of iot from the perspective of the observability of complex networks," Heliyon, 2024.

[4] A. Javadpour, F. Ja'fari, T. Taleb, Y. Zhao, Y. Bin, and C. Benzaïd, "Encryption as a service for iot: Opportunities, challenges and solutions," IEEE Internet of Things Journal, 2023.

[5] J. Feng, J. Wang, Y. Zhu, and K. Han, "A hybrid chaotic encryption asic with dynamic precision for internet of things," IEEE Internet of Things Journal, 2023.

[6] C. Zou, H. Li, X. Zhang, Y. Liu, Y. Shang, and C. Zhou, "Target localization image encryption of wind turbines based on dna strand replacement rule," Chaos, Solitons & Fractals, vol. 183, p. 114890, 2024.

[7] M. Es-sabry, N. El Akkad, L. Khrissi, K. Satori, W. El-Shafai, T. Altameem, and R. S. Rathore, "An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers," Egyptian Informatics Journal, vol. 25, p. 100449, 2024.

[8] Y. Dong, G. Zhao, Y. Ma, Z. Pan, and R. Wu, "A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata," Information Sciences, vol. 593, pp. 121–154, 2022.

[9] X. Wang and N. Guan, "Chaotic image encryption algorithm based on block theory and reversible mixed cellular automata," Optics & Laser Technology, vol. 132, p. 106501, 2020.

[10] A. Babaei, H. Motameni, and R. Enayatifar, "A new permutation-diffusion-based image encryption technique using cellular automata and dna sequence," Optik, vol. 203, p. 164000, 2020.

[11] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps," Optik, vol. 261, p. 169122, 2022.

[12] H. Zhang, X.-q. Wang, Y.-j. Sun, and X.-y. Wang, "A novel method for lossless image compression and encryption based on lwt, spiht and cellular automata," Signal Processing: Image Communication, vol. 84, p. 115829, 2020.

[13] Y. Wang, Y. Shang, Z. Shao, Y. Zhang, G. Coatrieux, H. Ding, and T. Liu, "Multiple color image encryption based on cascaded quaternion gyrator transforms," Signal Processing: Image Communication, p. 116793, 2022.

[14] Y. Zhang, R. Zhao, Y. Zhang, R. Lan, and X. Chai, "High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system," Journal of King Saud University-Computer and Information Sciences, 2022.

[15] M. Kaur and V. Kumar, "Beta chaotic map based image encryption using genetic algorithm," International Journal of Bifurcation and Chaos, vol. 28, no. 11, p. 1850132, 2018.

[16] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," Optics and Lasers in Engineering, vol. 51, no. 6, pp. 665–673, 2013.

[17] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," Journal of information security and applications, vol. 45, pp. 117–130, 2019.

[18] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," Neural Computing and Applications, vol. 32, no. 9, pp. 4961–4988, 2020.

[19] U. S. Choi, S. J. Cho, J. G. Kim, S. W. Kang, and H. D. Kim, "Color image encryption based on programmable complemented maximum length cellular automata and generalized 3-d chaotic cat map," Multimedia Tools and Applications, vol. 79, no. 31, pp. 22825–22842, 2020.

[20] P. K. Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," Nonlinear Dynamics, vol. 100, no. 3, pp. 2877–2898, 2020.

[21] Q. Lai, C. Lai, H. Zhang, and C. Li, "Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption," Chaos, Solitons & Fractals, vol. 158, p. 112017, 2022.

[22] S. Zhou, Z. Zhao, and X. Wang, "Novel chaotic colour image cryptosystem with deep learning," Chaos, Solitons & Fractals, vol. 161, p. 112380, 2022.

[23] Y. Khedmati, R. Parvaz, and Y. Behroo, "2d hybrid chaos map for image security transform based on framelet and cellular automata," Information Sciences, vol. 512, pp. 855–879, 2020.

[24] M. Yildirim, "Optical color image encryption scheme with a novel dna encoding algorithm based on a chaotic circuit," Chaos, Solitons & Fractals, vol. 155, p. 111631, 2022.

[25] S. Sun, "A novel hyperchaotic image encryption scheme based on dna encoding, pixel-level scrambling and bit-level scrambling," IEEE Photonics Journal, vol. 10, no. 2, pp. 1–14, 2018.

[26] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic dna encoding," IEEE Photonics Journal, vol. 10, no. 4, pp. 1–14, 2018.

[27] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," Signal Processing, vol. 164, pp. 163–185, 2019.

[28] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," Archives of Computational Methods in Engineering, vol. 27, no. 1, pp. 15–43, 2020.

[29] J. Von Neumann, A. W. Burks, et al., "Theory of self-reproducing automata," IEEE Transactions on Neural Networks, vol. 5, no. 1, pp. 3–14, 1966.

[30] S. Nandi, B. Kar, and P. P. Chaudhuri, "Theory and applications of cellular automata in cryptography," IEEE Transactions on computers, vol. 43, no. 12, pp. 1346–1357, 1994.

[31] D. R. Chowdhury, I. Sengupta, and P. P. Chaudhuri, "A class of two-dimensional cellular automata and their applications in random pattern testing," Journal of Electronic Testing, vol. 5, no. 1, pp. 67–82, 1994.

[32] S. Jafari, V.-T. Pham, S. M. R. H. Golpayegani, M. Moghtadaei, and S. T. Kingni, "The relationship between chaotic maps and some chaotic systems with hidden attractors," International Journal of Bifurcation and Chaos, vol. 26, no. 13, p. 1650211, 2016.

[33] P. R. Krishna, C. V. S. Teja, V. Thanikaiselvan, et al., "A chaos based image encryption using tinkerbell map functions," in 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 578–582, IEEE, 2018.

[34] T. A. Dhopavkar, S. K. Nayak, and S. Roy, "Ietd: a novel image encryption technique using tinkerbell map and duffing map for iot applications," Multimedia Tools and Applications, vol. 81, no. 30, pp. 43189–43228, 2022.

[35] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," Archives of Computational Methods in Engineering, pp. 1–29, 2018.

[36] X. Wang and N. Guan, "A novel chaotic image encryption algorithm based on extended zigzag confusion and rna operation," Optics & Laser Technology, vol. 131, p. 106366, 2020.

[37] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool, and M. Amin, "An efficient image encryption scheme based on chaotic and deoxyribonucleic acid sequencing," Mathematics and Computers in Simulation, vol. 177, pp. 441–466, 2020.

[38] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process," Multimedia systems, vol. 20, pp. 45–64, 2014.

[39] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," Communications in Nonlinear Science and Numerical Simulation, vol. 18, no. 11, pp. 3075–3085, 2013.

[40] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat, "Ievca: An efficient image encryption technique for iot applications using 2-d von-neumann cellular automata," Multimedia Tools and Applications, vol. 80, no. 21, pp. 31529–31567, 2021.

[41] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6d hyperchaotic and dna coding," Multimedia Tools and Applications, vol. 80, pp. 13841–13864, 2021.

[42] Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, M. A. Al Sibahee, V. O. Nyangaresi, D. G. Honi, A. I. Abdulsada, and X. Jiao, "Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map," IEEE Access, vol. 10, pp. 26257–26270, 2022.

[43] M. Shrivastava, S. Roy, K. Kumar, C. V. Pandey, and J. Grover, "Licca: a lightweight image cipher using 3-d cellular automata," Nonlinear Dynamics, vol. 106, no. 3, pp. 2679–2702, 2021.

[44] B. Ge, X. Chen, G. Chen, and Z. Shen, "Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation," IEEE Access, vol. 9, pp. 137635–137654, 2021.

[45] P. Ping, F. Xu, and Z.-J. Wang, "Image encryption based on non-affine and balanced cellular automata," Signal Processing, vol. 105, pp. 419–429, 2014.

[46] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, et al., A statistical test suite for

random and pseudorandom number generators for cryptographic applications, vol. 22. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2001.

B VIJAYA BHASKAR RAO is presently pursuing a Ph.D. at Manipal University in Jaipur. He completed his Master of Computer Applications (MCA) studies at Bharathidasan University in Tiruchirappalli in 1999. Cryptography and cybersecurity are his areas of interest. He works for the Government of India in Hyderabad at the National Informatics Centre (NIC). His work tackles important problems in the realm of digital security, emphasising the creation of sophisticated cryptographic techniques and strategies to fend off new online dangers.

UMASHANKAR RAWAT received his Ph.D. (Computer Science and Engineering) in Year 2013 from Jaypee University of Engineering and Technology, Guna in the area of Linux File System Security. In 2003, he graduated with an M.E. in computer engineering from SGSITS in Indore. He is currently employed with Manipal University in Jaipur as a professor in the CSE department. He published 36 research papers in SCI/Scopus journals and conference proceedings. He is an expert in cryptography and security.

SATYABRATA ROY is an Associate Professor in the Department of Computer Science and Engineering, School of Computing & Information Technology at Manipal University Jaipur, Rajasthan, India. He received his Ph.D. and M.Tech. (with honors) degrees in Computer Science and Engineering in 2020 and 2014 respectively; and B.Tech. in Information Technology in 2009. His research interests include Cryptography, Internet of Things, Cellular Automata, Computer Networks, Computational Intelligence, Machine Learning and Formal Languages. He is an enthusiastic and motivating technocrat with more than 10 years of research and academic experience at different reputed institutes. He has supervised many students for their M. Tech. dissertation work and currently supervising Ph.D. scholars at Manipal University Jaipur. He has published many research articles in top quality International Journals, National/ International conferences of repute. He is also working as reviewer for several reputed International Journals. He has served as member of technical program committee of many international conferences and symposiums. He has organized many international conferences, FDPs and Workshops. He has participated in many Short-Term Courses, Faculty Development Programmes, Workshops and MOOCs offered by prestigious universities of India and abroad. He has served as resource person of many FDPs and seminars. He is a senior member of IEEE and professional member of ACM.

CHAGGAN LAL is a cybersecurity researcher with a robust academic and professional background in critical infrastructure security, network security, and cloud cybersecurity. Currently engaged with the Critical Infrastructure Security and Resilience (CISaR) group at NTNU, Norway, his expertise spans over eight years of rigorous research and practical implementations in diverse areas of cybersecurity. He holds a Ph.D. in Computer Science and Engineering from Malaviya National Institute of Technology, Jaipur, India, where his research focused on enhancing the Quality of Experience for real-time video streaming in wireless networks. His academic journey is complemented by an M.Tech in Information Technology from IIIT Allahabad and a B.E. in Computer Science and Engineering from MBM Government Engineering College, Jodhpur. Throughout his career, Dr. Lal has contributed significantly to various high-impact research projects, including EU-H2020 funded initiatives and industry collaborations. In past, he worked at prestigious institutions such as TU Delft, University of Padova, and Simula Research Labs, where he has led efforts in network security, distributed ledger technologies, and cybersecurity for IoT networks. Moreover, his professional credentials include certifications such as Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP), and multiple Microsoft certifications in cybersecurity and cloud security domains.